DUMPSARENA

GIAC Certified Firewall Analyst

GIAC GCFW

Version Demo

Total Demo Questions: 34

Total Premium Questions: 347

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Volume A	165
Topic 2, Volume B	162
Total	347

QUESTION NO: 1

You work as a Security Manger for Tech Perfect Inc. The company has a Windows-based network.

You want to scroll real-time network traffic to a command console in a readable format.

Which of the following command line utilities will you use to accomplish the task?

A. WinPcap

B. WinDump

C. iptables

D. libpcap

ANSWER: B

Explanation:

WinDump is the appropriate utility because it is a Windows command-line packet-capture and analysis tool designed to display captured network traffic directly in a console. It provides tcpdump-style output, allowing an analyst to watch packets as they are received and apply capture filters to focus on relevant hosts, protocols, ports, or other packet characteristics. Its output is intended to be readable during live troubleshooting and security analysis, while captured traffic can also be written to a packet-capture file for later inspection.

On Windows, WinDump relies on a packet-capture driver to access network interfaces and receive packets. This makes it useful for the stated requirement: observing real-time network traffic interactively from a command prompt rather than configuring firewall rules or merely installing a capture library. For example, an analyst can run WinDump with no write-to-file argument to print packet summaries continuously to the console, or add protocol and host filters to reduce noise during an investigation. The WinDump project documentation describes it as a Windows version of tcpdump and provides usage details at WinDump for Windows. General packet-capture filter syntax and live-capture behavior are documented in the tcpdump manual page.

QUESTION NO: 2

You work as a Network Administrator for Blue Bell Inc. The company has a TCP-based network. The company has two offices in different cities. The company wants to connect the two offices by using a public network. You decide to configure a virtual private network (

VPN) between the offices. Which of the following protocols is used by VPN for tunneling?

A. HTTPS

B. SSL

C. IPSec

D. L2TP

ANSWER: D

Explanation:

L2TP is the correct answer because it is specifically a tunneling protocol designed to carry Layer 2 traffic across an intervening IP network. In a VPN deployment, L2TP creates a logical tunnel between the two endpoints, allowing traffic from one private network to traverse a public network as encapsulated tunnel traffic. This makes it suitable for linking geographically separated offices while preserving the logical connectivity required by the private network.

L2TP is defined by the IETF as a protocol for tunneling Layer 2 frames over packet-switched networks. In practical VPN architectures, it is commonly paired with IPsec: L2TP provides the tunnel mechanism, while IPsec provides authentication, integrity protection, and encryption for the traffic carried through that tunnel. Therefore, when the question asks specifically for the protocol used for VPN tunneling, L2TP is the most precise choice. The protocol specification is available in RFC

2661: Layer Two Tunneling Protocol (L2TP). Microsoft's overview of VPN deployments also describes L2TP/IPsec as a VPN technology combining L2TP tunneling with IPsec security.

QUESTION NO: 3

When client data is encapsulated into an LWAPP header, the wireless LAN controller improves the coverage areas. Which information does the wireless LAN controller check?

Each correct answer represents a part of the solution. Choose two.

A. CCA

B. SNR

C. WCS

D. RSSI

ANSWER: B D

Explanation:

The wireless LAN controller uses received signal strength indicator (RSSI) and signal-to-noise ratio (SNR) as key radio-frequency measurements when assessing client connectivity and making coverage-related decisions. RSSI represents the received power level of a wireless signal at the access point or client radio. It provides the controller with an indication of how strongly a client is being heard, which is fundamental when evaluating whether the client has sufficient signal coverage.

SNR complements RSSI by comparing the wanted wireless signal with the surrounding noise floor. A strong received signal alone is not enough for reliable wireless operation if environmental or radio interference is also high. By considering SNR, the controller can assess the usable quality of the RF connection and support appropriate client servicing and radio-management behavior. Together, RSSI and SNR provide the signal-level and signal-quality information needed to evaluate effective WLAN coverage.

Cisco documents RSSI and SNR as RF signal-quality metrics used in wireless client and radio monitoring. See Cisco Wireless Controller Configuration Guide and Cisco guidance on RSSI and SNR.

QUESTION NO: 4

Which of the following firewalls operates at three layers- Layer3, Layer4, and Layer5?

A. Application layer firewall

B. Proxy firewall

C. Dynamic packet-filtering firewall

D. Circuit-level firewall

ANSWER: C

Explanation:

Dynamic packet-filtering firewall is correct because it performs stateful inspection rather than making a decision solely from the fields in an individual packet. It evaluates network-layer addressing information at Layer 3 and transport-layer protocol, port, and TCP-control information at Layer 4. Crucially, it also maintains state for active communications: it records the connection or session context and uses that context to determine whether later packets belong to a valid, established flow. This session-awareness is the Layer 5 capability described in the question.

In practice, dynamic filtering creates and consults a state table. For example, once an outbound TCP connection is permitted and its handshake establishes the flow, returning packets can be allowed when they match the recorded session state. This makes the firewall's decisions dynamic: the permitted traffic depends on the currently tracked connection, including its

protocol, endpoints, ports, and state, rather than on a permanently static rule for every packet. NIST describes stateful inspection as tracking the state of network connections and using that information when filtering traffic; see NIST SP 800-41 Rev. 1. Cisco likewise describes stateful firewall operation as maintaining connection-state information for traffic flows; see Cisco: What Is a Firewall?.

QUESTION NO: 5

Which of the following IPv4 fields become obsolete while removing the hop-by-hop segmentation (fragmentation) procedure from the IP header?

Each correct answer represents a part of the solution. Choose three.

A. Fragment Offset field

B. Datagram Length field

C. Flags field

D. Datagram Identification Number field

ANSWER: A C D

Explanation:

IPv6 removes the IPv4 router-based, hop-by-hop fragmentation mechanism from its fixed base header. Consequently, the IPv4 *Fragment Offset field*, *Flags field*, and *Datagram Identification Number field* are not present in the IPv6 base header. In IPv4, these three fields work together to support fragmentation and reassembly: the identification value associates fragments with the same original datagram, the flags convey fragmentation control information, and the fragment offset identifies each fragment's position within the original packet. IPv6 routers do not fragment packets while forwarding them. Instead, an IPv6 source performs Path MTU Discovery and, when fragmentation is necessary, the source may include a separate Fragment extension header. That extension header carries fragmentation-specific information only for packets that actually require it, rather than placing those fields in every packet's fixed network-layer header. This design reduces routine forwarding-header processing and supports IPv6's simplified base-header format. See RFC 8200, Section 4.5 for IPv6 fragmentation requirements and the Fragment header, and RFC 791, Section 3.1 for the corresponding IPv4 header fields.

QUESTION NO: 6

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He is using a tool to crack the wireless encryption keys. The description of the tool is as follows:

Which of the following tools is John using to crack the wireless encryption keys?

A. Kismet

B. PsPasswd

C. AirSnort

D. Cain

ANSWER: C

Explanation:

AirSnort is the correct tool because it was specifically designed to recover Wired Equivalent Privacy encryption keys from captured wireless traffic. It operates passively, collecting a sufficient number of packets and analyzing the initialization vectors transmitted with vulnerable Wired Equivalent Privacy-protected frames. The tool is historically associated with attacks on the weaknesses in the RC4-based key-scheduling implementation used by Wired Equivalent Privacy. Once enough suitable traffic has been collected, AirSnort can attempt to derive the shared key, enabling an authorized security assessor to demonstrate that a legacy wireless network is insecure.

This makes AirSnort a classic wireless-encryption key-cracking utility in the context of ethical hacking and legacy wireless-security assessments. Its intended use aligns with evaluating whether an organization still relies on obsolete Wired Equivalent Privacy protections and documenting the resulting exposure so the organization can migrate to modern wireless security, such as WPA2 or WPA3 with strong authentication and encryption. The AirSnort project documentation describes its purpose as recovering Wired Equivalent Privacy keys from captured traffic: AirSnort Project. The practical process and the underlying weakness in Wired Equivalent Privacy are also described in the Aircrack-ng WEP-cracking documentation.

QUESTION NO: 7

Address Resolution Protocol (ARP) spoofing, also known as ARP poisoning or ARP Poison Routing (APR), is a technique used to attack an Ethernet wired or wireless network. ARP spoofing may allow an attacker to sniff data frames on a local area network (LAN), modify the traffic, or stop the traffic altogether. The principle of ARP spoofing is to send fake ARP messages to an Ethernet LAN.

What steps can be used as a countermeasure of ARP spoofing?

Each correct answer represents a complete solution. Choose all that apply.

A. Using ARP Guard utility

B. Using smash guard utility

C. Using static ARP entries on servers, workstation and routers

D. Using ARP watch utility

E. Using IDS Sensors to check continually for large amount of ARP traffic on local subnets

ANSWER: A C D E

Explanation:

Using ARP Guard utility, using static ARP entries on servers, workstation and routers, using ARP watch utility, and using IDS Sensors to check continually for large amount of ARP traffic on local subnets are valid defensive measures against ARP spoofing. ARP protection tools validate ARP-to-MAC bindings and can identify or block suspicious mapping changes. Static ARP mappings prevent a protected host from accepting an attacker's forged reply for critical peers such as the default gateway, making them particularly useful for small numbers of high-value systems.

ARPwatch provides ongoing visibility into unexpected Ethernet-address and IP-address association changes, allowing administrators to investigate and remediate poisoning attempts quickly. IDS monitoring similarly detects anomalous ARP behavior, including bursts of gratuitous replies or excessive ARP traffic, and can generate alerts for incident response. These detective controls are important because ARP has no built-in authentication and an attack may otherwise remain invisible. In managed switched networks, these host and monitoring measures should be complemented by switch enforcement such as Dynamic ARP Inspection, which validates ARP packets against trusted binding information. Cisco describes this validation approach in its Dynamic ARP Inspection documentation; ARPwatch behavior is documented in the ARPwatch manual page.

QUESTION NO: 8

Which of the following proxy servers is placed anonymously between the client and remote server and handles all of the traffic from the client?

A. Web proxy server

B. Open proxy server

C. Forced proxy server

D. Caching proxy server

ANSWER: C

Explanation:

A forced proxy server is correct because it is deployed so that client communications must traverse the proxy before reaching remote services. Rather than depending on each user or application to voluntarily select and configure a proxy, the network architecture or traffic-redirection policy places the proxy in the communication path and forces client traffic through it. This allows the organization to apply centralized inspection, authentication, access control, logging, filtering, and policy enforcement to the client's outbound connections. From the remote server's perspective, the proxy acts as the intermediary that establishes or relays the connection, while the client is not directly communicating with the destination in the normal end-to-end manner. This arrangement is especially useful where security controls must apply consistently to all managed client traffic and users must not be able to bypass the organization's proxy policy. The general proxy model—an intermediary that receives requests and forwards them to origin servers—is defined in RFC 9110, Section 3.7. Traffic interception and redirection techniques used to ensure flows pass through an intermediary are also described in RFC 3040.

QUESTION NO: 9

You work as a Network Administrator for NetTech Inc. Your manager needs to access a particular server on the network from outside the company network. You have a registered IP address assigned to a router on the company network. Which of the following will be useful for accessing the server from outside the network?

A. Overloading

B. Dynamic VLAN

C. Switch

D. Static NAT

ANSWER: D

Explanation:

Static NAT is the appropriate solution because it creates a fixed, one-to-one mapping between an internal server's private IP address and a publicly routable registered IP address. External users can then send traffic to that public address, and the edge router or firewall translates and forwards it to the designated internal server. This provides a stable, predictable address for services that must be reachable from outside the organization, such as a web, mail, or remote-access server.

In practice, the configuration must also include an access-control policy permitting only the required inbound protocol and port—for example, HTTPS on TCP port 443—and appropriate routing to the server. Network address translation does not itself provide access control; the firewall policy should limit exposure to the intended service and approved source networks where feasible. The registered address on the company router provides the public-facing endpoint needed for the static translation. Cisco's NAT overview describes static NAT as a permanent mapping between an inside local address and an inside global address: Cisco: NAT Order of Operation and Static NAT. NIST also recommends restricting externally accessible services and controlling traffic at network boundaries: NIST SP 800-41 Rev. 1, Guidelines on Firewalls and Firewall Policy.

QUESTION NO: 10

Which of the following information must the fragments carry for the destination host to reassemble them back to the original unfragmented state?

Each correct answer represents a complete solution. Choose all that apply.

A. MF flag

B. Length of the data

C. IP address

D. Offset field

E. MAC address

F. IP identification number

ANSWER: A B C D F

Explanation:

IPv4 fragmentation relies on fields in every fragment's IP header so the receiving host can associate fragments with the same original datagram, place their payloads in the proper sequence, and identify when the complete payload has arrived. The IP identification number provides a common identifier for all fragments of one original datagram. Source and destination IP addresses are also part of the reassembly context, ensuring that identification values are evaluated in association with the communicating endpoints; the IP protocol field is additionally part of the formal IPv4 reassembly key, although it is not offered here. The Offset field specifies where a fragment's data belongs relative to the beginning of the original payload, in units of eight bytes. The MF flag indicates whether additional fragments follow; a fragment with MF cleared identifies the final fragment. Finally, the IPv4 Total Length field allows a receiver to determine the size of the data carried by each individual fragment after accounting for its header length. Together, these values allow the receiver to collect, order, and validate the fragments before delivering the reconstructed datagram to the upper-layer protocol. RFC 791 defines the Identification, Flags, Fragment Offset, and Total Length header fields and their fragmentation behavior: RFC 791. RFC 815 further describes IPv4 fragment reassembly using source, destination, protocol, and identification information: RFC 815.

QUESTION NO: 11

You work as a technician for Tech Perfect Inc. You are troubleshooting an Internet name resolution issue. You ping your ISP ' s DNS server address and find that the server is down. You want to continuously *ping* the DNS address until you have stopped the command. Which of the following commands will you use?

A. ping -a

B. ping -l

C. ping -n

D. ping -t

ANSWER: D

Explanation:

`ping -t` is correct because, in the Windows `ping` utility, the `-t` parameter causes ICMP Echo Requests to continue indefinitely for the specified destination. This is useful during troubleshooting because it lets a technician monitor when a previously unreachable DNS server becomes reachable again, or observe intermittent connectivity while network conditions change. The command should include the DNS server's IP address or resolvable host name, for example, `ping -t 203.0.113.53`. The continuous test remains active until the technician manually interrupts it with `Ctrl+C`, which also displays cumulative ping statistics such as packets sent, received, lost, and round-trip timing. A technician can use `Ctrl+Break` to display statistics during an ongoing continuous ping without terminating the command. Microsoft documents `-t` as the option that specifies pinging the target until the process is interrupted. See the official Windows ping command documentation and Microsoft's Windows command reference.

QUESTION NO: 13 - (SIMULATION)

Fill in the blank with the appropriate tool name.

_____ is a network protocol analyzer tool that is used to capture packet data from an existing network or examine packet data from a pre-saved file.

ANSWER: See the explanation for the answer

Explanation:

Wireshark is the network protocol analyzer used to capture packet data from a live network interface or examine packets from a previously saved capture file.

Fill in the blank with: `Wireshark`.

QUESTION NO: 14

Which of the following commands is recommended by Cisco for latest switches and routers to erase the contents of NVRAM?

A. erase startup-config

B. write erase

C. erase nvram:

D. reload

ANSWER: A

Explanation:

`erase startup-config` is the recommended Cisco IOS command for removing the saved startup configuration from NVRAM on current Cisco switches and routers. The startup configuration is the configuration file read during device boot; deleting it returns the device to a state where it has no saved configuration to load at the next reload. This is commonly performed when decommissioning a device, preparing it for reassignment, or resetting a lab device before applying a new configuration.

Cisco IOS documentation identifies `erase startup-config` as the command used to erase the startup configuration and notes that it supersedes the older `write erase` form. After the configuration is erased, a reload is normally required for the device to start without the former saved configuration. Administrators should verify that any required configuration has been backed up before running the command, because the saved configuration cannot be restored unless a backup exists. Cisco's command reference documents this behavior in its Cisco IOS Fundamentals Command Reference; Cisco's configuration guidance also describes clearing the startup configuration before reloading a device: Cisco: Clearing a Cisco IOS Device Configuration.

QUESTION NO: 15

An IDS is a group of processes working together in a network. These processes work on different computers and devices across the network. Which of the following processes does an IDS perform?

Each correct answer represents a complete solution. Choose all that apply.

A. Event log analysis

B. Monitoring and analysis of user and system activity

C. Statistical analysis of abnormal traffic patterns

D. Network traffic analysis

ANSWER: A B C D

Explanation:

An intrusion detection system collects and evaluates information from networked hosts, security devices, and communications to identify signs of malicious activity or policy violations. **Event log analysis** is a core host-based IDS capability because operating-system, application, authentication, and audit records provide evidence of suspicious actions. **Monitoring and analysis of user and system activity** enables an IDS to identify behaviors such as unauthorized access attempts, privilege misuse, unexpected process execution, and changes to critical resources.

Statistical analysis of abnormal traffic patterns is also an IDS function, particularly for anomaly-based detection. A baseline of expected behavior can be used to identify meaningful deviations, including unusual volumes, connection patterns, protocols, or traffic timing. **Network traffic analysis** is fundamental to network-based IDS operation: sensors inspect packets, flows, headers, payloads where available, and protocol behavior to detect known signatures and suspicious activity. These functions may be distributed across sensors, collectors, management servers, and analysis components, which fits the description of an IDS as coordinated processes operating across network devices. NIST describes IDPS technologies as monitoring events occurring in computer systems and networks and analyzing them for signs of possible incidents; see NIST SP 800-94 and the CISA IDS/IPS overview.

QUESTION NO: 16

In which of the following situations does legal and authorized traffic cause an intrusion detection system (IDS) to generate an alert and slow down performance?

Each correct answer represents a complete solution. Choose all that apply.

A. False alert

B. False illusion

C. False generation

D. False positives

ANSWER: A D

Explanation:

False alert and false positives describe the condition in which an IDS identifies benign, legitimate activity as suspicious or malicious and generates an alert even though no actual security violation has occurred. This is commonly called a false positive (or false alarm). For example, normal application behavior, an approved administrative scan, or an unusual but authorized traffic pattern may match an IDS signature or exceed an anomaly threshold. The alert must then be recorded, transmitted, and potentially investigated, consuming IDS processing capacity as well as analyst time. At high volumes, false positives can create alert fatigue and reduce the effectiveness and perceived performance of the monitoring operation. NIST describes intrusion-detection technologies as mechanisms that monitor events and analyze them for signs of possible incidents; effective tuning and analysis are necessary because alerts may not represent genuine malicious activity. See NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems. The broader NIST incident-handling guidance also emphasizes validating and analyzing indicators before treating them as confirmed incidents: NIST SP 800-61 Rev. 2.

QUESTION NO: 18

Which of the following monitors program activities and modifies malicious activities on a system?

A. Back door

B. NIDS

C. HIDS

D. RADIUS

E. HIPS

ANSWER: E

Explanation:

HIPS is correct because a host-based intrusion prevention system monitors activity on an individual endpoint and can take action to prevent or disrupt detected malicious behavior. Host-based monitoring can observe events such as process execution, application behavior, system calls, changes to protected files or configuration, and other local security-relevant activity. Its prevention capability distinguishes it from detection-only monitoring: once a rule, signature, behavioral policy, or

other analytic identifies activity as hostile, the system can block the process, terminate it, prevent the action, quarantine an affected object, or otherwise alter the host security state to stop the activity.

NIST describes intrusion prevention capabilities as responding to detected threats by stopping attacks or changing the security environment, while host-based technologies collect and analyze activity from a single host. This directly matches the combination in the question of monitoring program activities and modifying malicious activity on the system. In modern endpoint-security products, these controls are often incorporated into endpoint detection and response platforms, but the specific traditional term for the stated function is a host-based intrusion prevention system. See NIST's Guide to Intrusion Detection and Prevention Systems (IDPS) and the CISA overview of intrusion detection and prevention systems.

QUESTION NO: 19

Which of the following can be used in an extended access list to filter traffic?

Each correct answer represents a part of the solution. Choose all that apply.

A. Destination MAC address

B. Source IP address

C. Protocol

D. Destination IP address

E. TCP or UDP port number

ANSWER: B C D E

Explanation:

Extended IP access control lists provide Layer 3 and Layer 4 traffic filtering. They can match a **Source IP address** and a **Destination IP address**, allowing a policy to control communication between particular hosts, subnets, or broader IP address ranges. Extended ACL entries also specify a **Protocol**, such as IP, TCP, UDP, ICMP, or another supported IP protocol. This enables policy enforcement based on the type of network traffic rather than only on its endpoints.

For TCP and UDP traffic, an extended ACL can additionally match a **TCP or UDP port number**. Port criteria identify the application service associated with the packet, such as HTTPS on TCP port 443 or DNS on UDP port 53. Depending on the ACL syntax and intended policy, the port match can apply to a source port, destination port, or a defined range. Combining source and destination addressing, protocol selection, and service-port criteria makes extended ACLs suitable for precise firewall filtering rules. Cisco's ACL documentation describes extended ACL entries as using protocol, source and destination addresses, and optional TCP/UDP port operators. See Cisco IOS IP Access List Configuration Guide and Cisco: Access Control List Examples.

QUESTION NO: 20

Sam works as a Network Administrator for Gentech Inc. He has been assigned a project to develop the rules that define the IDP policy in the rulebase. Which of the following will he define as the components of the IDP policy rule?

Each correct answer represents a complete solution. Choose all that apply.

A. IDP Profiler

B. IDP rule IP actions

C. IDP appliance deployment mode

D. IDP rule notifications

ANSWER: B D

Explanation:

An IDP policy rule must specify what the device does when traffic matches the rule and how administrators are informed about that event. **IDP rule IP actions** are therefore a core rule component. The action defines the enforcement behavior associated with a detected attack or matched traffic, such as allowing, dropping, closing, or otherwise responding to the session or packet according to the configured IDP policy. This makes the rule operational rather than merely descriptive.

IDP rule notifications are also a rule component because they define the alerting and reporting behavior tied to the rule. Notifications enable security personnel and management systems to receive relevant information about IDP events, supporting monitoring, incident handling, correlation, and auditing. An IDP deployment needs both an enforcement decision and a mechanism to communicate meaningful security events to operators. Juniper's IDP policy documentation describes policy rules as combining traffic and attack matching with configured actions and logging or notification behavior. See the Juniper IDP policy configuration documentation and the Juniper IDP overview for the role of IDP policy enforcement and event reporting.

QUESTION NO: 22

You work as a Firewall Analyst in the Tech Perfect Inc. The company has a Linux-based environment. You have installed and configured netfilter/iptables on all computer systems.

What are the main features of netfilter/iptables?

Each correct answer represents a complete solution. Choose all that apply.

A. It includes many plug-ins or modules in 'patch-o-matic' repository

B. It includes a number of layers of API's for third party extensions

C. It offers stateless and stateful packet filtering with both IPv4 and IPv6 addressing schemes

D. It provides network address and port address translations with both IPv4 and IPv6 addressing schemes

ANSWER: A B C

Explanation:

Netfilter/iptables is a modular Linux packet-processing framework. Its extensibility is reflected by the availability of numerous match, target, and protocol-related extensions; historically, the Patch-O-Matic collection was an important source of additional iptables patches and modules. This modular design permits administrators to tailor filtering and packet handling to operational requirements rather than relying on a fixed, minimal rule set.

The framework also exposes kernel hooks and interfaces that enable packet-processing components and third-party extensions to integrate with the networking stack. Netfilter processes traffic at defined points in the stack, while iptables provides the familiar userspace rule-management interface for configuring tables, chains, matches, and targets.

A core firewall capability is both stateless filtering, in which each packet is evaluated independently, and stateful filtering, in which connection tracking supplies context about flows and permits rules based on connection state. Netfilter/iptables supports filtering for both IPv4 and IPv6 through the appropriate protocol-family tooling and tables. These capabilities make it suitable for enforcing host-based policy across dual-stack Linux environments. The Linux kernel documentation describes Netfilter's hooks, connection tracking, and NAT architecture at Linux Kernel Netfilter documentation; the iptables project documentation is available at netfilter.org documentation.

QUESTION NO: 23

Which of the following address translation types only translates one (and only one) IP address to another without using ports?

A. NAT

B. Dynamic NAT

C. PAT

D. Static NAT

ANSWER: D

Explanation:

Static NAT is correct because it establishes a fixed, one-to-one mapping between a specific inside IP address and a specific outside IP address. Each configured internal host always translates to the same external address, and the translation is based on the network-layer address alone rather than on transport-layer port numbers. This makes static mappings appropriate when a host, such as a public-facing server, must be consistently reachable through a known public IP address.

In firewall and network-address-translation terminology, “static” describes the persistent nature of the mapping: the mapping is configured in advance and remains available regardless of whether the host currently has an active connection. The one-to-one relationship also means that a distinct public address is required for each internal address that needs its own static external identity. Cisco’s NAT configuration documentation describes static NAT as a permanent mapping between an inside local address and an inside global address, while its NAT overview distinguishes address-only translation from port-based translation. See Cisco IOS NAT Address Conservation and Cisco: NAT Order of Operation.

QUESTION NO: 24

Which of the following protocols is used with a tunneling protocol to provide security?

A. EAP

B. FTP

C. IPX/SPX

D. IPSec

ANSWER: D

Explanation:

IPSec is correct because it supplies the security services commonly paired with tunneling protocols, particularly Layer 2 Tunneling Protocol (L2TP). L2TP creates a tunnel for carrying traffic between endpoints, but the tunnel mechanism itself does not provide strong encryption, integrity protection, or peer authentication. IPSec adds those protections through its security associations and protocols, protecting packets in transit against disclosure and tampering while also authenticating the communicating peers. In a conventional L2TP/IPSec VPN deployment, IPSec is established first to protect the network path, and L2TP traffic then passes through that protected IPSec connection. This combination allows remote-access or site-to-site communications to use L2TP’s tunneling capabilities without exposing the encapsulated traffic. The Internet Engineering Task Force’s L2TP/IPSec specification explicitly describes using IPSec to secure L2TP traffic and defines the relevant transport-mode arrangement. See RFC 3193: Securing L2TP using IPSec. For further technical background on IPSec’s authentication, integrity, confidentiality, and key-management architecture, consult RFC 4301: Security Architecture for the Internet Protocol.

QUESTION NO: 25

You are the Network Administrator for a college. Wireless access is widely used at the college. You want the most secure wireless connections you can have. Which of the following would you use?

A. WPA

B. WPA2

C. WEP

ANSWER: B

Explanation:

WPA2 is the correct choice among the listed wireless-security technologies because it provides substantially stronger protection than the older WEP and WPA protocols. WPA2 uses the IEEE 802.11i security framework and supports AES-based CCMP encryption, which provides confidentiality, integrity protection, and stronger resistance to the practical cryptographic attacks that affected earlier wireless mechanisms. For a college deployment, WPA2 should ideally be implemented as WPA2-Enterprise, using 802.1X authentication and a RADIUS server. This gives each student, faculty member, and staff member an individual authenticated session rather than sharing a single wireless passphrase across the campus. It also enables centralized account lifecycle management and access revocation when users leave or devices are lost.

NIST's wireless-security guidance recommends enterprise authentication and strong cryptographic protections for organizational WLANs, including 802.1X-based access control and robust encryption. WPA2 with AES/CCMP was the established secure enterprise WLAN standard for the technologies represented in this question. In modern deployments, WPA3-Enterprise is preferable where supported, but it is not one of the available selections; therefore, WPA2 is the strongest applicable answer here. See NIST SP 800-153, Guidelines for Securing Wireless LANs and Wi-Fi Alliance security overview.

QUESTION NO: 26

What are the advantages of stateless autoconfigration in IPv6?

Each correct answer represents a part of the solution. Choose three.

A. No server is needed for stateless autoconfiguration.

B. No host configuration is necessary.

C. It provides basic authentication to determine which systems can receive configuration data

D. Ease of use.

ANSWER: A B D

Explanation:

IPv6 Stateless Address Autoconfiguration (SLAAC) allows a host to configure its own IPv6 address by combining a network prefix advertised in an ICMPv6 Router Advertisement with an interface identifier. Consequently, "No server is needed for stateless autoconfiguration." is correct: unlike stateful address assignment, SLAAC does not require a DHCP server to allocate and track individual addresses. Routers advertise the necessary on-link prefix and default-router information.

"No host configuration is necessary." is also correct in the usual operational sense that an IPv6-capable host can automatically create a usable address and install network parameters without an administrator manually entering an address, prefix length, gateway, or similar basic settings. This substantially reduces deployment effort, particularly on large or frequently changing networks.

"Ease of use." follows directly from this automatic, decentralized process. Hosts can join an IPv6 network and obtain basic connectivity with minimal infrastructure and administrative overhead. SLAAC also uses Duplicate Address Detection before an address is assigned for normal use, supporting safe automatic configuration. The defining SLAAC behavior and required processing are specified in RFC 4862; Router Advertisements are defined by RFC 4861.

QUESTION NO: 27

David works as the Security Manager for PassGuide Inc. He has been assigned a project to detect the attacks over multiple connections and sessions and to count the number of scanned ports in a defined time period. Which of the following rulebases will he use to accomplish the task?

A. Traffic Anomalies rulebase

B. Exempt rulebase

C. SYN Protector rulebase

D. Network Honeypot rulebase

ANSWER: A

Explanation:

Traffic Anomalies rulebase is correct because it is designed to identify suspicious behavior that becomes evident only when traffic is correlated across multiple connections or sessions. Port-scanning activity is a classic example: an attacker may generate many individually ordinary connection attempts, but the aggregate pattern—attempts to multiple destination ports against a host within a configured interval—indicates reconnaissance. Traffic-anomaly protections maintain the necessary context and thresholds to evaluate that cumulative behavior, including the number of distinct ports contacted during the relevant time window. This allows the firewall or intrusion-prevention system to recognize a scan even when no single connection alone is sufficient evidence of an attack. Such correlation-based detection is an important firewall-analysis capability because it distinguishes repeated, structured probing from normal isolated connection attempts. Check Point describes intrusion prevention as inspecting and preventing malicious network activity, including reconnaissance-related threats, in its Intrusion Prevention System overview. The correlation and analysis concepts assessed here also align with the network-security focus of the GIAC Certified Firewall Analyst certification.

QUESTION NO: 28

You want to create a binary log file using tcpdump. Which of the following commands will you use?

A. tcpdump -B

B. tcpdump -w capture.pcap

C. tcpdump -dd

D. tcpdump -d

ANSWER: B

Explanation:

`tcpdump -w capture.pcap` is the correct command because the `-w` flag tells tcpdump to write captured packets to a file rather than displaying packet summaries in the terminal. The output is saved in pcap format, a binary capture format that preserves packet data and associated capture metadata for later inspection. A filename must follow `-w`; in this example, the resulting file is named `capture.pcap`. The capture can subsequently be examined with tcpdump by using `tcpdump -r capture.pcap`, or opened in packet-analysis tools such as Wireshark. This workflow is important in firewall analysis and incident response because it permits analysts to retain evidence, revisit traffic after capture has stopped, apply different display filters during review, and share the same packet trace with other investigators. The tcpdump manual specifies that `-w` writes raw packets to a file for later analysis, rather than parsing and printing them as they are received. The pcap file format is also documented by the TCPDUMP/libpcap project. See the tcpdump manual page and the pcap savefile format documentation.

QUESTION NO: 29

Which of the following statements is true about ICMP packets?

Each correct answer represents a complete solution. Choose all that apply.

A. They are used to report errors if a problem in IP processing occurs.

B. They use UDP datagrams.

C. They guarantee the delivery of datagrams.

D. The PING utility uses them to verify connectivity between two hosts.

E. They are encapsulated within IP datagrams.

ANSWER: A D E

Explanation:

ICMP is an Internet-layer control and diagnostic protocol carried directly by IP. “They are used to report errors if a problem in IP processing occurs” is correct because ICMP defines error-reporting messages that communicate conditions encountered while processing or delivering IP packets. Examples include Destination Unreachable, Time Exceeded, and Parameter Problem messages. These messages give hosts and network devices useful feedback about forwarding and packet-processing outcomes.

“The PING utility uses them to verify connectivity between two hosts” is also correct. Ping normally sends ICMP Echo Request messages and evaluates returned ICMP Echo Reply messages. This provides a practical indication that a destination is reachable through the tested path and can respond at the IP layer; the reply timing is also commonly used to observe round-trip latency.

“They are encapsulated within IP datagrams” is correct because ICMP is assigned IP protocol number 1 and is transported as the payload of an IP packet. This placement lets routers and hosts exchange ICMP control information using the same network-layer addressing and routing infrastructure as ordinary IP traffic. RFC 792 specifies the original ICMP message format and its inclusion within IP datagrams, while the IANA protocol-number registry identifies ICMP as protocol 1. See RFC 792 and the IANA IP Protocol Numbers registry.

QUESTION NO: 30

Which of the following Linux file systems is a journaled file system?

A. ext3

B. ext2 C. ext

C. ext4

ANSWER: A

Explanation:

ext3 is a journaled Linux filesystem. It extends the earlier ext2 filesystem by adding a journal: a dedicated on-disk record of pending filesystem metadata updates. Before committing an operation such as creating, deleting, or renaming a file, ext3 records the relevant changes in that journal. If a system loses power or crashes during an update, the filesystem can replay or discard incomplete journal transactions during the next mount. This substantially reduces recovery time compared with a full filesystem consistency scan and helps keep filesystem structures consistent after an unclean shutdown.

Journaling is particularly valuable on systems that require predictable restart and recovery behavior. ext3 supports multiple journaling modes, including ordered mode, which journals metadata while arranging ordinary file-data writes before the associated metadata is committed. The Linux ext3 manual documents its journaling behavior and mount options, including the journal-related data modes. See the ext3 manual page and the Linux kernel filesystem documentation for additional technical details.

QUESTION NO: 31

Which of the following fields are specified when rules are created for the Network Honeypot

rulebase?

Each correct answer represents a complete solution. Choose all that apply.

A. A destination/service match condition

B. Detection settings

C. Operation mode

D. Response options

ANSWER: A C D

Explanation:

Network Honeypot rules are defined by the traffic to which the honeypot behavior applies and by the action the gateway takes when that traffic is seen. Therefore, *A destination/service match condition* is specified to identify the protected destination and service associated with the deceptive, unused, or otherwise monitored network exposure. *Operation mode* is also a rule field because it determines how the Network Honeypot protection operates for matching traffic, such as whether the rule is used in a detection-oriented or enforcement-oriented mode. *Response options* are specified as well, allowing the administrator to configure the resulting handling and notification behavior for honeypot events. Together, these fields provide the match criteria, operational behavior, and response behavior required for an effective Network Honeypot rule. This design reflects the broader firewall-policy principle that a rule must define both the traffic selection conditions and the action or response applied to matching traffic. Check Point's documentation portal provides the product administration and Threat Prevention guidance underlying Network Honeypot policy configuration: Check Point Product Documentation. For related firewall-policy concepts, see Check Point: What Is a Firewall Rule?.

QUESTION NO: 33

You work as a Network Administrator for Tech Perfect Inc. The company has a TCP/IPbased routed network. Two routers have been configured on the network. A router receives a packet. Which of the following actions will the router take to route the incoming packet?

Each correct answer represents a part of the solution. Choose two.

A. Use the routing table to determine the best path to the destination network address.

B. Read the destination IP address.

C. Add the path covered by the packet to the routing table.

D. Read the source IP address.

E. Use the routing table to determine the best path to the source network address.

ANSWER: A B

Explanation:

Routers forward an incoming Internet Protocol packet by first examining its destination Internet Protocol address. That destination address identifies the network or host toward which the packet must be delivered; it is the address used for the forwarding decision. After obtaining the destination address, the router consults its routing table and selects the most appropriate matching route, ordinarily using longest-prefix matching. The selected route supplies the forwarding information, including the next hop or outgoing interface, that allows the router to send the packet toward its destination. These steps are fundamental to connectionless Internet Protocol forwarding: each router makes an independent forwarding decision for each received packet based on the packet's destination and locally available forwarding information. The Internet Engineering Task Force's router requirements describe route selection as determining the best route for a destination, while Cisco's routing documentation explains that a router uses the destination address and routing table to choose a path. See RFC 1812: Requirements for IP Version 4 Routers and Cisco: Routing Basics.

QUESTION NO: 34

Peter works as a Computer Hacking Forensic Investigator. He has been called by an organization to conduct a seminar to give necessary information related to sexual harassment within the work place. Peter started with the definition and types of sexual harassment. He then wants to convey that it is important that records of the sexual harassment incidents should be maintained, which helps in further legal prosecution. Which of the following data should be recorded in this documentation?

Each correct answer represents a complete solution. Choose all that apply.

A. Names of the victims

B. Location of each incident; Nature of harassment

C. Date and time of incident

ANSWER: A B C

Explanation:

Records should identify the people affected by the reported conduct, so *Names of the victims* is necessary information. Accurate identification permits an organization to contact the reporting individual, provide support and anti-retaliation protections, compare related reports, and preserve a reliable factual record for an internal investigation or later legal proceeding. The *Location of each incident* and *Nature of harassment* should also be documented because these facts establish what conduct is alleged and the context in which it occurred. Location may identify relevant workplace conditions, records, cameras, or potential witnesses, while a clear description of the conduct allows investigators to assess the report consistently and determine an appropriate response. Finally, the *Date and time of incident* creates a usable chronology. A timeline helps investigators locate contemporaneous communications, schedules, access records, and other potentially relevant evidence, while also supporting a prompt and thorough investigation. The U.S. Equal Employment Opportunity Commission advises employers to establish effective complaint procedures and investigate harassment complaints promptly and thoroughly. Its enforcement guidance also emphasizes the importance of gathering relevant facts when addressing harassment reports. See the EEOC Enforcement Guidance on Harassment in the Workplace and the EEOC harassment overview.